EXHIBIT B

Providing Foreign Malign Influence Threat Information to Social Media Platforms

In executing its mission to keep the American people safe, the Department of Justice has prioritized countering foreign malign influence operations, including online operations.

One of the ways the FBI supports this mission is by providing foreign malign influence (FMI) threat information to companies hosting social media (Social Media Platforms) so that they may, based on their independent judgment, initiative, and decision-making process, take steps to mitigate such threats.[1]

It is also Department of Justice "policy to alert the victims and unwitting targets of foreign influence activities, when appropriate and consistent with the Department's policies and practices, and with our national security interests."[2] One of the appropriate reasons for disclosing FMI threat information is, as outlined in the Justice Manual, "to alert technology companies or other private sector entities to foreign influence operations when their services are used to disseminate covert foreign government propaganda or disinformation, or to provide other covert support to political organizations or groups."[3]

When a company receives FMI threat information from the FBI, it is entirely up to the company whether to take any action based on the shared information. Any actions that companies may take in response to receiving information from the FBI in these contexts are strictly voluntary and are based on their independent judgment, initiative, and decision-making process.

In 2019, bipartisan majorities of Congress recognized the threat to national security posed by FMI in Title 50, Section 3369 of the United States Code titled, “Cooperative Actions to Detect and Counter Foreign Influence Operations,” which includes the finding that foreign actors have used the platforms provided by technology companies to engage in FMI activities that threaten U.S. national security, and will likely continue to do so. Specifically, Congress found that:

> Any actions the companies may take in response to receiving FMI threat information from the FBI in this context are strictly voluntary and are based on their independent judgment, initiative, and/or decision making processes.

> (1) [a hostile power deployed] information warfare against the United States, its allies and partners, with the goal of advancing the strategic interests of the [hostile power] . . . (2) One line of effort deployed as part of these information warfare operations is the weaponization of social media platforms with the goals of intensifying societal tensions, undermining trust in governmental institutions within the United States, its allies and partners in the West, and generally sowing division, fear, and confusion. (3) These information warfare operations are a threat to the national security of the United States and that of the allies and partners of the United States. As former Director of National Intelligence Dan Coats stated, “These actions are persistent, they are pervasive and they are meant to undermine America’s democracy . . .” (7) Because these information warfare operations are deployed within and across private social media platforms, the companies that own these platforms have a responsibility to detect and facilitate the removal or neutralization of foreign adversary networks operating clandestinely on their platforms.

Congress stated in the same section that “it is the sense of Congress that information from law enforcement and the intelligence community is also important in assisting efforts by these social media companies to identify foreign information warfare operations.”

Since well before those Congressional findings, the Department of Justice, acting through the FBI, has been working to combat FMI threats. In the fall of 2017, the FBI established

the FBI's Foreign Influence Task Force (FITF) as a multi-division FBI section comprised of operational and analytical personnel to combat FMI operations targeting U.S. democratic institutions.

One of FITF's key lines of effort has been to "[l]ead the engagement with social media and Internet technology providers" to enable an effective dialogue with Social Media Platforms focused on understanding the capabilities of these providers, and providing information to these platforms for the companies to use, if they choose to do so within their discretion, in furtherance of self-monitoring and mitigation efforts.

The FBI has implemented standard operating procedures (SOP) by which the FBI transmits FMI threat information to Social Media Platforms. The SOP are designed to continue to ensure that Americans' First Amendment rights are being protected while the hidden hand of foreign malign threat actors is being exposed. These procedures govern instances in which an FBI employee seeks to share information regarding specific activities or accounts relating to FMI, such as particular posts or uploads of videos, with Social Media Platforms. An overview of the SOP is set forth below.

Pursuant to the SOP, FBI employees may share information with a Social Media Platform regarding specific activities or accounts relating to FMI in the following circumstances:

> "It is the sense of Congress that information from law enforcement and the intelligence community is also important in assisting efforts by these social media companies to identify foreign information warfare operations."
>
> 50 U.S. Code § 3369

1. The employee determines that the activities are being conducted covertly by, on behalf of, or pursuant to instruction from a foreign government and/or actor and in support of an FMI operation;

2. The employee identifies specific, credible, and articulable facts that provide high confidence for assessing that the activity is attributed to a foreign government, foreign nonstate actor, or their proxy engaged in FMI; and

3. All communications to and with the Social Media Platform are made in a way that makes clear that: (a) the FBI is not asking the Platform to take any action in response to the sharing of the information, and the Platform has no obligation to do so, (b) the FBI is not asking the Platform to change or amend its terms of service, (c) the FBI does not investigate solely based on First Amendment-protected activity, and (d) no adverse action will be taken by the FBI based on the Platform's decision about whether or how to respond to the information being shared.

These interactions are voluntary, and the FBI shall always respect a Social Media Platform's decision whether or not to participate.

---

[1] See U.S. Department of Justice, Report of the Attorney General's Cyber Digital Task Force (2018), available at justice.gov/archives/ag/page/file/1076696/download, at 12 ("[T]he FBI and [Intelligence Community] partners may be able to identify and track foreign agents as they establish their infrastructure and mature their online presence, in which case authorities can work with social media companies to illuminate and ultimately disrupt those agents' activities through voluntary removal of accounts that violate a company's terms of service.").

[2] Justice Manual § 9-90.730 – Disclosure of Foreign Influence Operations.

[3] *Id.*

ViCAP

FBI Jobs

Submit a Tip

Crime Statistics

History

FOIPA

Scams & Safety

FBI Kids

News

Stories

Videos

Press Releases

Speeches

Testimony

Podcasts and Radio

Photos

Español

Apps

How We Can Help You

Law Enforcement

Victims

Parents and Caregivers

Students

Businesses

Safety Resources

Need an FBI Service or More Information?

What We Investigate

Terrorism

Counterintelligence
Cyber Crime
Public Corruption
Civil Rights
Organized Crime
White-Collar Crime
Violent Crime
WMD

About

Mission & Priorities
Leadership & Structure
Partnerships
Community Outreach
FAQs

Contact Us

Field Offices
FBI Headquarters
Visit the FBI Experience
Overseas Offices

Additional Resources

Accessibility
eRulemaking
Freedom of Information / Privacy Act
Legal Notices
Legal Policies & Disclaimers
Privacy Policy
USA.gov
White House
No FEAR Act
Equal Opportunity

FBI

FEDERAL BUREAU
OF INVESTIGATION

FBI.gov Contact Center